DOCUMENTO OFICIAL LICITATÓRIO Nº 397/2020

EDITAL Nº 107/2020 - PREGÃO ELETRÔNICO - OBJETO: “Contratação de empresa para Gestão e Governança em conformidade com a LGPD - Lei Geral de Proteção de Dados - Lei nº 13.709/2018 como Serviço, em consonância com as especificações constantes neste documento e seus anexos.”

ATA DE RESPOSTA DO PEDIDO DE ESCLARECIMENTO

Aos vinte e dois dias do mês de maio do ano de dois mil e vinte, na sala de licitações da Secretaria Municipal das Licitações, sito na Rua Frei Orlando, 68, térreo, Canoas (RS), reuniu-se o pregoeiro designado pelo Decreto n.º 139/2019 e sua equipe de apoio, para responder o pedido de esclarecimento da empresa AGILITY, na pessoa do Sr. Gustavo Camini - Coordenador – Regional Sul - Arquiteto de Soluções encaminhado ao pregoeiro pelo e-mail pregaoeletronico@canoas.rs.gov.br. Foi solicitado o que segue: **Prezado Senhor Pregoeiro,** Seguem nossos questionamentos referentes ao **EDITAL Nº 107/2020 - PREGÃO ELETRÔNICO**. Objeto: “Contratação de empresa para Gestão e Governança em conformidade com a LGPD - Lei Geral de Proteção de Dados – Lei nº 13.709/2018 como Serviço. **1. Questionamentos iniciais:** Sobre a volumetria de dados, qual seria a quantidade de dados estimada em Terabytes para o total do ambiente? Existem aplicações a serem analisadas além das previstas no edital? Por exemplo: Office 365, GDrive, Dropbox, etc. A informação das 18 unidades está centralizada ou pulverizada entre as unidades? Sobre os itens do edital, temos os seguintes questionamentos: **2. Item 2 - Atividades consultivas Questionamento 01:**
Sobre o item 3.1.2 A quantidade de 3.000 horas é uma estimativa. Os pagamentos serão feitos conforme a utilização mensal efetiva. Entendemos que ao final do mês, serão computadas as horas técnicas trabalhadas e será realizado o respectivo faturamento. Está correto o nosso entendimento? **Questionamento 02:** Sobre o item 3.1.3, em se tratando de atividades in-loco. **Quais são as respectivas localidades das secretarias? Questionamento 03:** Sobre o item 3.2.1 e subsequentes, o número de áreas de negócio, processos de negócio, workshops a serem realizados e colaboradores que participarão é fundamental para o correto dimensionamento do serviço. **Quais são as respectivas quantidades? Questionamento 04:** Sobre o item 3.2.3 no tocante ao inventário de ambientes tecnológicos e dados. Entendemos que essa entrega pode ser automatizada e contínua através da ferramenta, realizando uma varredura em dados estruturados e não estruturados. **Está correto o nosso entendimento? Questionamento 05:** Sobre o item 3.2.3. é possível nos informar um tamanho aproximado do ambiente? Quantidade de servidores, bancos de dados, sistemas, fileservers, serviços de armazenamento em nuvem, etc. são informações importantes para dimensionarmos o serviço. **Questionamento 06:** Sobre o item 3.2.3, no tocante a "Realização de varredura no ambiente tecnológico/Teste de Penetração", quantos e quais são os alvos (Aplicações e/ou IPs)? Estas informações são de suma importância para o dimensionamento do serviço, considerando o pentest como um serviço manual a ser executado por um Ethical Hacker devidamente capacitado. **Questionamento 07:** Sobre o item 2.2.3, no tocante a revisão de contratos, é possível nos fornecer uma estimativa da quantidade de contratos a serem analisados? **Questionamento 08:** Sobre o item 3.2.3 no tocante a "Criação e disseminação por canais digitais e ambientes físicos comuns de material de capacitação, workshop e EAD sobre LGPD". Entendemos

que o contratante irá fornecer os ambientes de disseminação e EAD, além dos insumos necessários para criação dos canais e design dos materiais. **Está correto o nosso entendimento? Questionamento 09:** Sobre o item 3.2.3, sobre os materiais de capacitação, workshop e EAD. **Qual a quantidade de apresentações e treinamentos que deverão ser elaborados? 3. Item 3 - Solução de orquestração Questionamento 10:** No item "3.1.4.1. A possibilidade de implantar a solução de Gestão e Governança em LGPD on-premises em Datacenter da Prefeitura sem limitação de usuários ou de processadores para uso por todos da área institucional da Prefeitura de Canoas". Entendemos que a solução que provenha um gerenciamento centralizado em plataforma SAAS, porém, com gateways que analisam os dados criando apenas trilhas da informação, sem a necessidade da cópia do arquivo para nossa solução atende ao item. **Está correto nosso entendimento? Questionamento 11:** Sobre o item e seus sub-intens"3.3.4.9 Inventário de Ativos de Dados que utilizam dados pessoais com o apontamento". Entendemos que a solução que provenha maneiras tecnológicas para realizar o "Data Mapping" e "Data Liking", categorizando registro com seus dados pessoais, possuindo parâmetros de ajustes de suas bases legais e com inúmeras detecções automatizadas com a possibilidade de desenvolvimento de detectores específicos para atender a vossa finalidade atenderá os requisitos. **Está correto nosso entendimento? Questionamento 12:** Sobre o item "3.3.4.12 Gestão de ocorrências de violação de dados pessoais." Entendemos que a solução deve prover um mecanismo de comunicação entre o titular e o DPO em momento de crise, que pode ocorrer através de um portal único e individual de cada usuário, podendo esse ser acionado através de tickets abertos atenderá os requisitos. **Está correto nosso entendimento? Questionamento 13:** Entendemos que, sobre o item 3.3.4.13. Gestão de transferência internacional de dados pessoais. Entendemos que solução que permita adicionar esses detalhes em um fluxo de mapa de dados de maneira que isso venha descrito no mapeamento atende ao item. **Está correto nosso entendimento? Questionamento 14:** Sobre o item 3.3.4.14. Gestão de compartilhamento de dados pessoais. Entendemos que uma solução que forneça o data map process e que nele seja possível adicionar em que momento você envia esses dados ou processa de maneira visual atende ao requisito. **Está correto nosso entendimento? Questionamento 15:** Sobre o item 3.3.4.17. Emissão de Plano de Ação para conformidade com a LGPD. Entendemos que a solução que permita a criação, edição ou importação de assessments para departamentos/vendors, de maneira que através desses assessments as áreas / vendors envolvidos, saibam se estão aderentes ou não a legislação, atende ao requerimento. **Está correto nosso entendimento? Questionamento 16:**
Sobre o item 3.3.4.16.” recomendações para controlar a gestão de conformidade com a LGPD”, uma ferramenta contendo um módulo de self-assessment ou assessment com terceiros atende ao requerimento. **Nosso entendimento está correto? Questionamento 17:** Sobre o item 3.3.4.21, entendemos que a solução que provenha uma maneira de acompanhamento sobre o assessment que está ligado ao plano de ação da empresa, trazendo uma maneira unificada onde o DPO poderá entrar em contato de maneira centralizada e em "Real time" com o DPO, sendo assim acompanhando o real time sobre o processo elaborado, atende ao item. **Está correto nosso entendimento? Questionamento 18:** Sobre o item 3.3.4.25, entendemos que a solução que provenha de uma maneira centralizada, um help com toda a documentação necessária para conexão com API atenderá ao item. **Está correto nosso entendimento? Questionamento 19:**
Sobre o item 3.3.4.26 “A solução deve ter barramento de Integração – ESB/SOA para integrar com os sistemas internos da Prefeitura, inclusive notificações e eventos automatizado”. É possível nos informar para qual finalidade será utilizado este barramento de integrações? Perguntamos, pois, em caso de integração com uma ferramenta de gerenciamento de tickets, nossa solução oferece todo processo de gestão e automação de demandas para atendimento às requisições dos titulares, não

havendo necessidade de abertura de tickets para TI, por exemplo. Neste caso, não haveria necessidade deste tipo de integração. Gostaríamos de entender como essa arquitetura está sendo utilizada e qual o propósito. Uma solução que provenha o gerenciamento de chamados e notificações de maneira automatizada atende ao item. **Está correto nosso entendimento? Questionamento 20:** Sobre o item "3.3.4.27. A solução deve arquitetura web em 3 camadas com persistência de dados em banco de dados relacional, servidor de middleware para hospedar a aplicação e camada de visão em HTML 5 responsivo".
Entendemos que a solução que provenha de uma arquitetura similar, porém, que a solução esteja em uma plataforma SAAS, não onerando a arquitetura do cliente, apenas se necessário a utilização de gateways de registro on-premises, atendem ao item. **Está correto nosso entendimento? Questionamento 21:** Sobre o item 3.3.5.1. Entendemos que uma solução baseada em SaaS comercializada através de subscrição anual atende ao requerimento. **Está correto nosso entendimento? Questionamento 22:** Sobre o item 3.3.5.8.1. Fornecer a referência completa do canal de atendimento e suporte técnico do produto ofertado, com o telefone 0800 ou ligação local (DDD 51) e e-mail do(s) responsável(is) técnico(s) que possa(m) responder questionamentos sobre todas as características do produto em pauta. Entendemos que atendendo aos itens 6.1.7.2.1. e 14.2.1. este canal de atendimento e suporte poderá ser da licitante. **Está correto o nosso entendimento?** O pregoeiro em análise a solicitação informa que a mesma foi remetida a área técnica da secretaria requisitante para manifestação, oportunidade na qual o Sr. Lino Roque Camargo Kieling - Superintendência Executiva Canoastec manifestou o que segue: 1.1. Questionamentos iniciais Sobre a volumetria de dados, qual seria a quantidade de dados estimada em Terabytes para o total do ambiente? R. Atualmente, a CANOASTEC gerencia, aproximadamente, 150 Terabytes de informações. Porém, está previsto, no serviço, um inventario onde esse número poderá aumentar. Existem aplicações a serem analisadas além das previstas no edital, por exemplo: office 365, GDrive, Drpbox, etc.? R. Certamente sim. Isto será visto durante o inventário. A informação das 18 unidades está centralizada ou pulverizada entre as unidades? R. A solução contratada não deve oferecer limitação de volumetria, uma vez que a volumetria irá variar bastante entre as unidades, além de ocorrer crescimento destes volumes de forma assimétrica entre as unidades. Além disto, as informações estão pulverizadas entre as unidades. 1.2. Atividades consultivas Questionamento 01: Sobre o item 3.1.2 A quantidade de 3.000 horas é uma estimativa. Os pagamentos serão feitos conforme a utilização mensal efetiva. Entendemos que ao final do mês, serão computadas as horas técnicas trabalhadas e será realizado o respectivo faturamento. Está correto o nosso entendimento? R. Sim. Questionamento 02: Sobre o item 3.1.3, em se tratando de atividades in-loco. Quais são as respectivas localidades das secretarias? R. Município de Canoas Questionamento 03: Sobre o item 3.2.1 e subsequentes, o número de áreas de negócio, processos de negócio, workshops a serem realizados e colaboradores que participarão é fundamental para o correto dimensionamento do serviço. Quais são as respectivas quantidades?
R. A quantidade de áreas de negócio, processos, workshops a serem realizados serão parâmetros para definir o quantitativo de horas de determinada OS. O item 3.2.1 admite o consumo incremental a partir de várias OS (sob demanda), assim não há necessidade destas informações para definição do preço dos serviços. Neste momento deve-se informar o valor unitário da hora de consultoria e o valor total, que é o valor da hora de consultoria multiplicado por 3000 horas. Lembrando-se, que não há compromisso no consumo de todas as 3000 horas. Questionamento 04: Sobre o item 3.2.3 no tocante ao inventário de ambientes tecnológicos e dados. Entendemos que essa entrega pode ser automatizada e contínua através da ferramenta, realizando uma varredura em dados estruturados e não estruturados. Está correto o nosso entendimento? R. A atividade é automatizada. Não há

necessidade de ser contínuo, mas não deve haver limitação de quantitativo de itens de inventário, nem de quantas vezes poderá ser executado. Questionamento 05: Sobre o item 3.2.3. é possível nos informar um tamanho aproximado do ambiente? Quantidade de servidores, bancos de dados, sistemas, fileservers, serviços de armazenamento em nuvem, etc. são informações importantes para dimensionarmos o serviço. R. O dimensionamento de serviço ocorre no momento de abertura de OS e como os serviços são sob demanda, não há necessidade de apontar dimensão neste momento. Quanto à licenciamento de ferramenta, não deve haver limitação de quantitativo de servidores, bancos de dados, sistemas, fileservers, armazenamento em nuvem e demais itens. Isto se dá em razão da dinamicidade dos ambientes de cada unidade negócio da prefeitura e da presença imprevisível de dados pessoais em cada um destes ativos de TI, impossibilitando a limitação no licenciamento. Questionamento 06: Sobre o item 3.2.3, no tocante a "Realização de varredura no ambiente tecnológico/Teste de Penetração", quantos e quais são os alvos (Aplicações e/ou IPs)? Estas informações são de suma importância para o dimensionamento do serviço, considerando o pentest como um serviço manual a ser executado por um Ethical Hacker devidamente capacitado. R. Trata-se de serviço a ser executado por OS. No momento da OS, será dimensionada a quantidade de alvos e então calculado o valor da OS, considerando esta métrica. Em tempo de contratação, necessitamos que seja apontado o valor da hora de consultoria. Questionamento 07: Sobre o item 2.2.3, no tocante a revisão de contratos, é possível nos fornecer uma estimativa da quantidade de contratos a serem analisados? R.Trata-se de serviço a ser executado por OS. No momento da OS será dimensionado a quantidade de contratos e então calculado o valor da OS, considerando esta métrica. Em tempo de contratação, necessitamos que seja apontado o valor da hora de consultoria. Questionamento 08: Sobre o item 3.2.3 no tocante a "Criação e disseminação por canais digitais e ambientes físicos comuns de material de capacitação, workshop e EAD sobre LGPD". Entendemos que o contratante irá fornecer os ambientes de disseminação e EAD, além dos insumos necessários para criação dos canais e design dos materiais. Está correto o nosso entendimento? R. Parcialmente correto. A apresentação em slides, design dos materiais e a capacitação deverão ser fornecidos pela empresa contratada. A plataforma deverá ser alguma de mercado tais como ZOOM, HANGOUT. Questionamento 09: Sobre o item 3.2.3, sobre os materiais de capacitação, workshop e EAD. Qual a quantidade de apresentações e treinamentos que deverão ser elaborados? R. Será informado no momento de OS e será levado em conta para determinar a quantidade de horas. 1.3.Solução de orquestração Questionamento 10: No item "3.1.4.1. A possibilidade de implantar a solução de Gestão e Governança em LGPD on-premises em Datacenter da Prefeitura sem limitação de usuários ou de processadores para uso por todos da área institucional da Prefeitura de Canoas". Entendemos que a solução que provenha um gerenciamento centralizado em plataforma SAAS, porém, com gateways que analisam os dados criando apenas trilhas da informação, sem a necessidade da cópia do arquivo para nossa solução atende ao item. Está correto nosso entendimento? R. Deverá ser permitido à CANOASTEC instalar a solução localmente em suas dependências, sem limitação de usuário ou processador em modelo SaaS, mas on-premises. Assim, o arquivo executável da solução (EAR, WAR, JAR, dentre outros que se fizerem necessários) deverão ser disponibilizados no ambiente local de servidores da CANOASTEC. Questionamento 11: Sobre o item e seus sub-intens"3.3.4.9 Inventário de Ativos de Dados que utilizam dados pessoais com o apontamento". Entendemos que a solução que provenha maneiras tecnológicas para realizar o "Data Mapping" e "Data Liking", categorizando registro com seus dados pessoais, possuindo parâmetros de ajustes de suas bases legais e com inúmeras detecções automatizadas com a possibilidade de desenvolvimento de detectores específicos para atender a vossa finalidade atenderá os requisitos. Está correto nosso entendimento? R. Apenas “Data Mapping”, não será necessário “Data Link”. O data mapping

deverá permitir a indicação de base legal por parte do DPO. O desenvolvimento de detectores é parte da funcionalidade e das evoluções do fornecedor da ferramenta, a CANOASTEC não pretende ter a possibilidade de desenvolver detectores personalizados, mas precisa ser capaz de configurar a regras de detecção, ou utilizando expressões regulares, ou dicionários de termos. Questionamento 12: Sobre o item "3.3.4.12 Gestão de ocorrências de violação de dados pessoais." Entendemos que a solução deve prover um mecanismo de comunicação entre o titular e o DPO em momento de crise, que pode ocorrer através de um portal único e individual de cada usuário, podendo esse ser acionado através de tickets abertos atenderá os requisitos. Está correto nosso entendimento? R. A solução não terá obrigatoriedade de gerenciar tickets de atendimento. A CANOASTEC já possui sistema de gestão de tickets de atendimento para isto. Este requisito prevê manter um cadastro na solução dos incidentes, de forma que o DPO possa consultar todos os incidentes que já ocorreram, as providencias tomadas, sem ter de recorrer a utilização de outra ferramenta para isto. O barramento de integração requisitado também nesta contratação como parte da solução poderá integrar o sistema de gestão de atendimento da CANOASTEC com este cadastro de incidentes da solução, evitando dupla digitação. Questionamento 13: Entendemos que, sobre o item 3.3.4.13. Gestão de transferência internacional de dados pessoais. Entendemos que solução que permita adicionar esses detalhes em um fluxo de mapa de dados de maneira que isso venha descrito no mapeamento atende ao item. Está correto nosso entendimento? R. Sim, atende. Portanto que seja possível incluir novos mapeamentos com o passar do tempo, atualizar estes fluxos. Questionamento 14: Sobre o item 3.3.4.14. Gestão de compartilhamento de dados pessoais. Entendemos que uma solução que forneça o data map processo e que nele seja possível adicionar em que momento você envia esses dados ou processa de maneira visual atende ao requisito. Está correto nosso entendimento? R. O requisito é até mais simples, é o registro de com quais operadores de dados pessoais os conjuntos de dados pessoais são compartilhados. Não é necessário indicar ou acompanhar cada data/evento em que ocorreu um evento de compartilhamento. É apenas o registro de quais compartilhamentos são realizados com terceiros. Questionamento 15: Sobre o item 3.3.4.17. Emissão de Plano de Ação para conformidade com a LGPD. Entendemos que a solução que permita a criação, edição ou importação de assessments para departamentos/vendors, de maneira que através desses assessments as áreas / vendors envolvidos, saibam se estão aderentes ou não a legislação, atende ao requerimento. Está correto nosso entendimento? R. Não. São dois artefatos diferentes. O assessment é um diagnóstico de situação e de gaps. O Plano de Ação é um cadastro de atividades do que deve ser feito para obter aderência à LGPD com responsável, data de início e fim, % de conclusão, status e descrição da atividade. Questionamento 16: Sobre o item 3.3.4.16. “recomendações para controlar a gestão de conformidade com a LGPD”, uma ferramenta contendo um módulo de self-assessment ou assessment com terceiros atende ao requerimento. Nosso entendimento está correto? R. Sim. Portanto, que esteja sob o conceito de solução integrada, que o usuário não precise se autenticar duas vezes (SSO - login único) e que estejam integrados via API e/ou barramento de integração. Questionamento 17: Sobre o item 3.3.4.21, entendemos que a solução que provenha uma maneira de acompanhamento sobre o assessment que está ligado ao plano de ação da empresa, trazendo uma maneira unificada onde o DPO poderá entrar em contato de maneira centralizada e em "Real time" com o DPO, sendo assim acompanhando o real time sobre o processo elaborado, atende ao item. Está correto nosso entendimento? R. Sim, está correto o entendimento. Questionamento 18: Sobre o item 3.3.4.25, entendemos que a solução que provenha de uma maneira centralizada, um help com toda a documentação necessária para conexão com API atenderá ao item. Está correto nosso entendimento? R. Sim. Recomendamos que haja um link para a documentação Swagger das API. Questionamento 19: Sobre o item 3.3.4.26 “A solução deve ter

barramento de Integração – ESB/SOA para integrar com os sistemas internos da Prefeitura, inclusive notificações e eventos automatizado". É possível nos informar para qual finalidade será utilizado este barramento de integrações? Perguntamos, pois, em caso de integração com uma ferramenta de gerenciamento de tickets, nossa solução oferece todo processo de gestão e automação de demandas para atendimento às requisições dos titulares, não havendo necessidade de abertura de tickets para TI, por exemplo. Neste caso, não haveria necessidade deste tipo de integração. Gostaríamos de entender como essa arquitetura está sendo utilizada e qual o propósito. Uma solução que provenha o gerenciamento de chamados e notificações de maneira automatizada atende ao item. Está correto nosso entendimento? R. O pedido por barramento de integração é para possibilitar a integração de quaisquer funcionalidades da solução com os sistemas e dados internos e externos das unidades de negócio. O barramento de dados é útil para consultar o catálogo de ativos de dados pessoais, o tipo de consentimento, os dados pessoais inventariados por sistema, o consumo da configuração de consentimento em tempo real entre os sistemas e a solução, dentre várias outras potencialidades que não apenas ticket de suporte. A solução será o catálogo de dados pessoais corporativo, desta forma é importante que este catálogo seja passível de fácil integração em qualquer cenário de negócio que trate dados pessoais. A existência de um barramento possibilita esta integração sem ser invasivo para os sistemas de origem e destino. Questionamento 20: Sobre o item "3.3.4.27. A solução deve arquitetura web em 3 camadas com persistência de dados em banco de dados relacional, servidor de middleware para hospedar a aplicação e camada de visão em HTML 5 responsivo". Entendemos que a solução que provenha de uma arquitetura similar, porém, que a solução esteja em uma plataforma SAAS, não onerando a arquitetura do cliente, apenas se necessário a utilização de gateways de registro on-premises, atendem ao item. Está correto nosso entendimento? R. Poderá ser SaaS, mas em infraestrutura local da CANOASTEC. Observe o item 3.1.4.1. A possibilidade de implantar a solução de Gestão e Governança em LGPD onpremises em Datacenter da Prefeitura sem limitação de usuários ou de processadores para uso por todos da área institucional da Prefeitura de Canoas. As unidades contam com dados sensíveis e como haverá descoberta de dados pessoais e a sua gestão, a decisão de segurança é não operar na nuvem pública e sim on-premises. Questionamento 21: Sobre o item 3.3.5.1. Entendemos que uma solução baseada em SaaS comercializada através de subscrição anual atende ao requerimento. Está correto nosso entendimento? R. Poderá ser SaaS, mas em infraestrutura local da CANOASTEC. Observe o item 3.1.4.1. A possibilidade de implantar a solução de Gestão e Governança em LGPD onpremises em Datacenter da Prefeitura sem limitação de usuários ou de processadores para uso por todos da área institucional da Prefeitura de Canoas. Questionamento 22: Sobre o item 3.3.5.8.1. Fornecer a referência completa do canal de atendimento e suporte técnico do produto ofertado, com o telefone 0800 ou ligação local (DDD 51) e e-mail do(s) responsável(is) técnico(s) que possa(m) responder questionamentos sobre todas as características do produto em pauta. Entendemos que atendendo aos itens 6.1.7.2.1. e 14.2.1. este canal de atendimento e suporte poderá ser da licitante. Está correto o nosso entendimento? R. Questão não entendida. O pregoeiro em acolhimento a manifestação técnica providencia a publicidade da presente Ata no DOMC e no site do Banrisul. Nada mais havendo digno de registro encerra-se a presente ata.

Silvio Renato Sandmann
Pregoeiro